

Union Calendar No. 139

105TH CONGRESS
1ST Session

H. R. 1903

[Report No. 105-243]

A BILL

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

SEPTEMBER 3, 1997

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

Union Calendar No. 139

105TH CONGRESS
1ST SESSION

H. R. 1903

[Report No. 105-243]

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 17, 1997

Mr. SENSENBRENNER (for himself, Mr. BROWN of California, Mrs. MORELLA, Mr. GORDON, Mr. DAVIS of Virginia, Ms. STABENOW, Mr. EHLERS, Ms. JACKSON-LEE of Texas, Mr. SESSIONS, Mr. PICKERING, Mr. TRAFICANT, Mr. COOK, and Mr. CANNON) introduced the following bill; which was referred to the Committee on Science

SEPTEMBER 3, 1997

Additional sponsors: Mr. GUTKNECHT, Mr. BRADY, Mrs. TAUSCHER, Mr. WELDON of Pennsylvania, Mr. LAMPSON, Mr. FOLEY, Mr. ENGLISH of Pennsylvania, Mr. DAN SCHAEFER of Colorado, Mr. DOYLE, Mr. BARCIA, Mr. CAPPS, Mr. EWING, Mr. BARTLETT of Maryland, Ms. RIVERS, Mr. ROHRBACHER, Mr. ROEMER, and Mr. NETHERCUTT

SEPTEMBER 3, 1997

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italic*]

[For text of introduced bill, see copy of bill as introduced on June 17, 1997]

A BILL

To amend the National Institute of Standards and Tech-

nology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
 2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 *This Act may be cited as the “Computer Security*
 5 *Enhancement Act of 1997”.*

6 **SEC. 2. FINDINGS AND PURPOSES.**

7 *(a) FINDINGS.—The Congress finds the following:*

8 *(1) The National Institute of Standards and*
 9 *Technology has responsibility for developing stand-*
 10 *ards and guidelines needed to ensure the cost-effective*
 11 *security and privacy of sensitive information in Fed-*
 12 *eral computer systems.*

13 *(2) The Federal Government has an important*
 14 *role in ensuring the protection of sensitive, but un-*
 15 *classified, information controlled by Federal agencies.*

16 *(3) Technology that is based on the application*
 17 *of cryptography exists and can be readily provided by*
 18 *private sector companies to ensure the confidentiality,*
 19 *authenticity, and integrity of information associated*
 20 *with public and private activities.*

21 *(4) The development and use of encryption tech-*
 22 *nologies should be driven by market forces rather than*
 23 *by Government imposed requirements.*

1 (5) *Federal policy for control of the export of*
 2 *encryption technologies should be determined in light*
 3 *of the public availability of comparable encryption*
 4 *technologies outside of the United States in order to*
 5 *avoid harming the competitiveness of United States*
 6 *computer hardware and software companies.*

7 (b) *PURPOSES.—The purposes of this Act are to—*

8 (1) *reinforce the role of the National Institute of*
 9 *Standards and Technology in ensuring the security of*
 10 *unclassified information in Federal computer systems;*

11 (2) *promote technology solutions based on pri-*
 12 *vate sector offerings to protect the security of Federal*
 13 *computer systems; and*

14 (3) *provide the assessment of the capabilities of*
 15 *information security products incorporating cryptog-*
 16 *raphy that are generally available outside the United*
 17 *States.*

18 **SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MANAGE-**
 19 **MENT INFRASTRUCTURE.**

20 *Section 20(b) of the National Institute of Standards*
 21 *and Technology Act (15 U.S.C. 278g–3(b)) is amended—*

22 (1) *by redesignating paragraphs (2), (3), (4),*
 23 *and (5) as paragraphs (3), (4), (7), and (8), respec-*
 24 *tively; and*

1 (2) by inserting after paragraph (1) the follow-
 2 ing new paragraph:

3 “(2) upon request from the private sector, to as-
 4 sist in establishing voluntary interoperable standards,
 5 guidelines, and associated methods and techniques to
 6 facilitate and expedite the establishment of non-Fed-
 7 eral management infrastructures for public keys that
 8 can be used to communicate with and conduct trans-
 9 actions with the Federal Government;”.

10 **SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NET-**
 11 **WORKS.**

12 Section 20(b) of the National Institute of Standards
 13 and Technology Act (15 U.S.C. 278g–3(b)), as amended by
 14 section 3 of this Act, is further amended by inserting after
 15 paragraph (4), as so redesignated by section 3(1) of this
 16 Act, the following new paragraphs:

17 “(5) to provide guidance and assistance to Fed-
 18 eral agencies in the protection of interconnected com-
 19 puter systems and to coordinate Federal response ef-
 20 forts related to unauthorized access to Federal com-
 21 puter systems;

22 “(6) to perform evaluations and tests of—

23 “(A) information technologies to assess
 24 security vulnerabilities; and

1 “(B) commercially available security prod-
2 ucts for their suitability for use by Federal agen-
3 cies for protecting sensitive information in com-
4 puter systems;”.

5 **SEC. 5. COMPUTER SECURITY IMPLEMENTATION.**

6 Section 20 of the National Institute of Standards and
7 Technology Act (15 U.S.C. 278g–3) is further amended—
8 (1) by redesignating subsections (c) and (d) as
9 subsection (f) and (g), respectively; and
10 (2) by inserting after subsection (b) the following
11 new subsection:

12 “(c) In carrying out subsection (a)(3), the Institute
13 shall—

14 “(1) emphasize the development of technology-
15 neutral policy guidelines for computer security prac-
16 tices by the Federal agencies;

17 “(2) actively promote the use of commercially
18 available products to provide for the security and pri-
19 vacy of sensitive information in Federal computer
20 systems; and

21 “(3) participate in implementations of
22 encryption technologies in order to develop required
23 standards and guidelines for Federal computer sys-
24 tems, including assessing the desirability of and the
25 costs associated with establishing and managing key

1 *recovery infrastructures for Federal Government in-*
 2 *formation.”.*

3 **SEC. 6. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**
 4 **AND INFORMATION.**

5 *Section 20 of the National Institute of Standards and*
 6 *Technology Act (15 U.S.C. 278g–3), as amended by this Act,*
 7 *is further amended by inserting after subsection (c), as*
 8 *added by section 5 of this Act, the following new subsection:*

9 *“(d)(1) The Institute shall solicit the recommendations*
 10 *of the Computer System Security and Privacy Advisory*
 11 *Board, established by section 21, regarding standards and*
 12 *guidelines that are being considered for submittal to the*
 13 *Secretary of Commerce in accordance with subsection*
 14 *(a)(4). No standards or guidelines shall be submitted to the*
 15 *Secretary prior to the receipt by the Institute of the Board’s*
 16 *written recommendations. The recommendations of the*
 17 *Board shall accompany standards and guidelines submitted*
 18 *to the Secretary.*

19 *“(2) There are authorized to be appropriated to the*
 20 *Secretary of Commerce \$1,000,000 for fiscal year 1998 and*
 21 *\$1,030,000 for fiscal year 1999 to enable the Computer Sys-*
 22 *tem Security and Privacy Advisory Board, established by*
 23 *section 21, to identify emerging issues related to computer*
 24 *security, privacy, and cryptography and to convene public*
 25 *meetings on those subjects, receive presentations, and pub-*

lish reports, digests, and summaries for public distribution
on those subjects.”.

**SEC. 7. EVALUATION OF CAPABILITIES OF FOREIGN
ENCRYPTION.**

Section 20 of the National Institute of Standards and
Technology Act (15 U.S.C. 278g–3), as amended by this Act,
is further amended by inserting after subsection (d), as
added by section 6 of this Act, the following new subsection:

“(e)(1) If the Secretary has imposed, or proposes to
impose, export restrictions on a product that incorporates
encryption technologies, the Institute may accept technical
evidence from the commercial provider of the product offered
to indicate that encryption technologies, embodied in the
form of software or hardware, that are offered and generally
available outside the United States for use, sale, license, or
transfer (whether for consideration or not) provide stronger
participation for privacy of computer data and trans-
missions of information in digital form than the encryption
technologies incorporated in the commercial provider’s
product.

“(2) Within 30 days after accepting technical evidence
from a commercial provider under paragraph (1), the Insti-
tute shall evaluate the accuracy and completeness of the
technical evidence and transmit to the Secretary, and to
the Committee on Science of the House of Representatives

1 *and the Committee on Commerce, Science, and Transpor-*
2 *tation of the Senate, a report containing the results of that*
3 *evaluation. The Institute may obtain assistance from other*
4 *Federal and private sector entities in carrying out evalua-*
5 *tions under this paragraph.*

6 “(3) Not later than 180 days after the date of the en-
7 actment of the Computer Security Enhancement Act of
8 1997, the Institute shall develop standard procedures and
9 tests for determining the capabilities of encryption tech-
10 nologies, and shall provide information regarding those pro-
11 cedures and tests to the public.

12 “(4) The Institute may require a commercial provider
13 seeking evaluation under this subsection to follow proce-
14 dures and carry out tests developed by the Institute pursu-
15 ant to paragraph (3).”.

16 **SEC. 8. LIMITATION ON PARTICIPATION IN REQUIRING**
17 **ENCRYPTION STANDARDS.**

18 *Section 20 of the National Institute of Standards and*
19 *Technology Act (15 U.S.C. 278g–3), as amended by this Act,*
20 *is further amended by adding at the end the following new*
21 *subsection:*

22 “(h) The Institute shall not promulgate, enforce, or
23 otherwise adopt standards, or carry out activities or poli-
24 cies, for the Federal establishment of encryption standards

1 *required for use in computer systems other than Federal*
 2 *Government computer systems.”.*

3 **SEC. 9. MISCELLANEOUS AMENDMENTS.**

4 *Section 20 of the National Institute of Standards and*
 5 *Technology Act (15 U.S.C. 278g–3), as amended by this Act,*
 6 *is further amended—*

7 *(1) in subsection (b)(8), as so redesignated by*
 8 *section 3(1) of this Act, by inserting “to the extent*
 9 *that such coordination will improve computer secu-*
 10 *rity and to the extent necessary for improving such*
 11 *security for Federal computer systems” after “Man-*
 12 *agement and Budget)”;*

13 *(2) in subsection (f), as so redesignated by sec-*
 14 *tion 5(1) of this Act, by striking “shall draw upon”*
 15 *and inserting in lieu thereof “may draw upon”;*

16 *(3) in subsection (f)(2), as so redesignated by sec-*
 17 *tion 5(1) of this Act, by striking “(b)(5)” and insert-*
 18 *ing in lieu thereof “(b)(8)”;* and

19 *(4) in subsection (g)(1)(B)(i), as so redesignated*
 20 *by section 5(1) of this Act, by inserting “and com-*
 21 *puter networks” after “computers”.*

22 **SEC. 10. FEDERAL COMPUTER SYSTEM SECURITY TRAIN-**
 23 **ING.**

24 *Section 5(b) of the Computer Security Act of 1987 (49*
 25 *U.S.C. 759 note) is amended—*

1 (1) by striking “and” at the end of paragraph
2 (1);

3 (2) by striking the period at the end of para-
4 graph (2) and inserting in lieu thereof “; and”; and

5 (3) by adding at the end the following new para-
6 graph:

7 “(3) to include emphasis on protecting sensitive
8 information in Federal databases and Federal com-
9 puter sites that are accessible through public net-
10 works.”.

11 **SEC. 11. COMPUTER SECURITY FELLOWSHIP PROGRAM.**

12 There are authorized to be appropriated to the Sec-
13 retary of Commerce \$250,000 for fiscal year 1998 and
14 \$500,000 for fiscal year 1999 for the Director of the Na-
15 tional Institute of Standards and Technology for fellow-
16 ships, subject to the provisions of section 18 of the National
17 Institute of Standards and Technology Act (15 U.S.C.
18 278g–1), to support students at institutions of higher learn-
19 ing in computer security. Amounts authorized by this sec-
20 tion shall not be subject to the percentage limitation stated
21 in such section 18.

22 **SEC. 12. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE**
23 **NATIONAL RESEARCH COUNCIL.**

24 (a) REVIEW BY NATIONAL RESEARCH COUNCIL.—Not
25 later than 90 days after the date of the enactment of this

1 *Act, the Secretary of Commerce shall enter into a contract*
2 *with the National Research Council of the National Acad-*
3 *emy of Sciences to conduct a study of public key infrastruc-*
4 *tures for use by individuals, businesses, and government.*

5 (b) *CONTENTS.—The study referred to in subsection*
6 *(a) shall—*

7 (1) *assess technology needed to support public*
8 *key infrastructures;*

9 (2) *assess current public and private plans for*
10 *the deployment of public key infrastructures;*

11 (3) *assess interoperability, scalability, and integ-*
12 *egrity of private and public entities that are elements*
13 *of public key infrastructures;*

14 (4) *make recommendations for Federal legisla-*
15 *tion and other Federal actions required to ensure the*
16 *national feasibility and utility of public key infra-*
17 *structures; and*

18 (5) *address such other matters as the National*
19 *Research Council considers relevant to the issues of*
20 *public key infrastructure.*

21 (c) *INTERAGENCY COOPERATION WITH STUDY.—All*
22 *agencies of the Federal Government shall cooperate fully*
23 *with the National Research Council in its activities in car-*
24 *rying out the study under this section, including access by*

1 properly cleared individuals to classified information if
 2 necessary.

3 (d) *REPORT.*—Not later than 18 months after the date
 4 of the enactment of this Act, the Secretary of Commerce
 5 shall transmit to the Committee on Science of the House
 6 of Representatives and the Committee on Commerce,
 7 Science, and Transportation of the Senate a report setting
 8 forth the findings, conclusions, and recommendations of the
 9 National Research Council for public policy related to pub-
 10 lic key infrastructures for use by individuals, businesses,
 11 and government. Such report shall be submitted in unclassi-
 12 fied form.

13 (e) *AUTHORIZATION OF APPROPRIATIONS.*—There are
 14 authorized to be appropriated to the Secretary of Commerce
 15 \$450,000 for fiscal year 1998, to remain available until ex-
 16 pended, for carrying out this section.

17 **SEC. 13. PROMOTION OF NATIONAL INFORMATION SECU-**
 18 **RITY.**

19 The Under Secretary of Commerce for Technology
 20 shall—

21 (1) promote the more widespread use of applica-
 22 tions of cryptography and associated technologies to
 23 enhance the security of the Nation's information in-
 24 frastructure;

1 (2) *establish a central clearinghouse for the col-*
 2 *lection by the Federal Government and dissemination*
 3 *to the public of information to promote awareness of*
 4 *information security threats; and*

5 (3) *promote the development of the national,*
 6 *standards-based infrastructure needed to support com-*
 7 *mercial and private uses of encryption technologies*
 8 *for confidentiality and authentication.*

9 **SEC. 14. DIGITAL SIGNATURE INFRASTRUCTURE.**

10 (a) *NATIONAL POLICY PANEL.*—*The Under Secretary*
 11 *of Commerce for Technology shall establish a National Pol-*
 12 *icy Panel for Digital Signatures. The Panel shall be com-*
 13 *posed of nongovernment and government technical and legal*
 14 *experts on the implementation of digital signature tech-*
 15 *nologies, individuals from companies offering digital signa-*
 16 *ture products and services, State officials, including offi-*
 17 *cials from States which have enacted statutes establishing*
 18 *digital signature infrastructures, and representative indi-*
 19 *viduals from the interested public.*

20 (b) *RESPONSIBILITIES.*—*The Panel established under*
 21 *subsection (a) shall serve as a forum for exploring all rel-*
 22 *evant factors associated with the development of a national*
 23 *digital signature infrastructure based on uniform standards*
 24 *that will enable the widespread availability and use of digi-*
 25 *tal signature systems. The Panel shall develop—*

1 (1) *model practices and procedures for certifi-*
2 *cation authorities to ensure accuracy, reliability, and*
3 *security of operations associated with issuing and*
4 *managing certificates;*

5 (2) *standards to ensure consistency among juris-*
6 *dictions that license certification authorities; and*

7 (3) *audit standards for certification authorities.*

8 (c) *ADMINISTRATIVE SUPPORT.—The Under Secretary*
9 *of Commerce for Technology shall provide administrative*
10 *support to the Panel established under subsection (a) of this*
11 *section as necessary to enable the Panel to carry out its*
12 *responsibilities.*

13 **SEC. 15. SOURCE OF AUTHORIZATIONS.**

14 *Amounts authorized to be appropriated by this Act*
15 *shall be derived from amounts authorized under the Na-*
16 *tional Institute of Standards and Technology Authorization*
17 *Act of 1997.*